IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

PLAINTIFFS' RESPONSE TO STATE DEFENDANTS'
NOTICE OF SUPPLEMENTAL AUTHORITY

On October 18, 2023, State Defendants filed a Notice of Supplemental Authority, contending that the Ninth Circuit's recent decision in *Lake v. Fontes*, No. 22-16413, 2023 WL 6800710 (9th Cir. Oct. 16, 2023) (per curiam), supports State Defendants' Motions for Summary Judgment. (Dkts. 1701, 1701-1.) State Defendants' Notice disappointingly misstates the *Lake* decision.

Perhaps most egregiously, State Defendants represent that "[t]he plaintiffs in *Lake* . . . sought relief barring the use of Arizona's electronic *voting* system in future Arizona elections." (Dkt. 1701 at 1 (emphasis added).) Not so. The *Lake* plaintiffs instead "sought to bar the use of electronic *tabulation* systems" to tabulate votes cast on *hand-marked paper ballots*. 2023 WL 6800710, at *1-2. In other words, the *Lake* plaintiffs challenged the very system that Plaintiffs here,

their experts, Defendants' own expert Ben Adida, and nearly the entirety of the election security community support today—i.e., hand-marked paper ballots tabulated by electronic scanners. Thus, the resolution of that case is no surprise and has no bearing on the facts and issues in this case.

Particularly important to the *Lake* court's finding on standing was that the plaintiffs there—unlike this case—"d[id] not contend that any electronic tabulation machine in Arizona has ever been hacked" and that "the hardware components of electronic tabulation systems are [] stored in secure locations." 2023 WL 6800710, at *2. This is literally the *opposite* of the facts of *this* case. As they did in their meritless summary judgment motions, State Defendants continue to take a head-in-the-sand approach to the breaches of Georgia's voting system—*in its operational environment*—via the Coffee County elections office and their own repeated and routine security failings. The facts of those breaches are undisputed and include:

> (i) unfettered access to Georgia's voting system by numerous individuals day after day over a period of weeks, including accessing and imaging virtually every machine and device that was used in elections both before *and after* the breaches;
>
> (ii) material changes to at least the county EMS server and the ICC scanner settings specifically to tinker with and test the software in ways that remain unclear, including, for example, changing the internal clock to trick the system into believing it was November 2020 Election Day during the breach; and
>
> (iii) theft of Dominion's proprietary software used in Georgia, which

> was then broadly disseminated via the Internet and hard drives distributed by mail.

(Dkt. 1636, MSJ Opp. at 14-25.)

This Court may recall that when Plaintiffs sought access for their experts to Georgia's BMD-based voting equipment and software in the summer of 2020, State Defendants insisted that such limited and heavily-controlled access—even under the protections of this Court's Protective Order—would present untenable risk for future elections in Georgia. They even demanded that any such access occur only at their own facility under lock and key and their watchful eyes, along with other extreme security measures. State Defendants' efforts now to dismiss the breach in Coffee County as unimportant ring hollow and contradict the Secretary's own Chief Information Officer's testimony that dissemination of the proprietary software used on Georgia's BMDs would provide a "roadmap" to hack Georgia elections. (MSJ Opp. at 2, 20.) That roadmap has been broadly available for years, and State Defendants have not identified or implemented new security measures to avoid a repeat of the breach in Coffee County—neither have State Defendants held anyone responsible for that breach to date.[1] State Defendants

[1] Three individuals charged by the Fulton County District Attorney's Office with crimes associated with the Coffee County caper have now pleaded guilty, and one of them reportedly has pled to at least one felony. Marshall Cohen et al., *Kenneth Chesebro: Pro-Trump lawyer pleads guilty in Georgia election subversion case,*

have not even begun an investigation of the security implications, failure of administration controls, or potential mitigation measures in the 34 months since the first breach occurred. They also have refused to implement the critical security measures CISA recommended they adopt "as soon as possible" in June 2022, well over a year ago. During 2023, the State Election Board declined to adopt State Election Board Rules formally proposed by CGG to mandate security incident reporting and mitigation to help avoid such breaches and define necessary action steps. As a result, similar breaches can occur without reporting to the State or any requirements to mitigate such breaches.

Moreover, in *Lake*, the court found that the plaintiffs relied "on a 'long chain of hypothetical contingencies' that have never occurred in Arizona," including "the specific voting equipment used in Arizona must have 'security failures' that allow a malicious actor to manipulate vote totals." 2023 WL 6800710, at *4. Here, however, Plaintiffs have established *many* such "security failures," including exactly how they "allow a malicious actor to manipulate vote totals" if exploited in Georgia (including by a voter in a voting booth in mere minutes), as detailed in Dr.

---

implicates Trump in fake elector conspiracy, CNN (Oct. 20, 2023), https://www.cnn.com/2023/10/20/politics/kenneth-chesebro-georgia-election-subversion.

Halderman's July 2021 Report, among other evidence compiled by Plaintiffs. State Defendants' own expert, Dr. Juan Gilbert, does not dispute these findings.

State Defendants omit other key differences that were central to the court's standing finding in *Lake*. For example, the *Lake* court emphasized that *after* an election, Arizona conducts "a sample hand count of the paper ballots" and "additional logic and accuracy testing" on the machines. 2023 WL 6800710, at *2. Georgia law does not mandate either. The *Lake* court also emphasized that Arizona's electronic tabulation equipment was secured with tamper-resistant seals and that the system could not be connected to the internet, wireless devices, or external networks, or contain remote access capabilities. *Id*. at *2.

In contrast, Plaintiffs have shown here that, *inter alia*, BMDs and other electronic devices used in Georgia elections often have been left unlocked, unsealed, unsupervised, and unsecured; Georgia CES Director Michael Barnes repeatedly has directed county elections supervisors to use BMDs for voting even though the BMDs' seals had been removed or were missing or broken; Barnes also directed counties to use with Georgia's BMD system the same removable media previously used with the state's antiquated DRE system, which was twice compromised by a white-hat hacker and which this Court enjoined from future use as unconstitutional; Georgia's BMD system relies on the *same* Internet-facing

computers long-used in 159 counties, including transmitting election results from each county to the state via the Internet; and the Secretary's own cybersecurity consultant (serving as his Chief Information Security Officer), Fortalice Solutions, repeatedly has found, year after year, serious security failings with the Secretary's information technology systems that Fortalice was able to exploit to gain full administrator access to those systems. (MSJ Opp. at 12-13, 36; Dkt. 1636, SAF Nos. 32, 55-65, 70, 227-242.)

State Defendants' claim that "Georgia has similar safeguards" as those in Arizona (Dkt. 1701 at 2), as described in *Lake*, ignores the voluminous evidence in the record here refuting that claim and showing that Georgia's physical and procedural safeguards repeatedly have failed to protect the system's integrity.[2] And because Arizona uses hand-marked paper ballots—rather than BMD-generated ballots that use QR codes for tabulation, as in Georgia—that system necessarily does not contain the many security design flaws and actual failures that pervade Georgia's current voting system. Those many serious failures are real and

[2] Arizona law also mandates more robust post-election audits than Georgia law. *See*, *e.g.*, Ariz. Rev. Stat. 16-602(B) & (F) (providing for the audits of the greater of two precincts or two percent of precincts in a county at random, for "up to five contested races," selected at random).

present here, not merely "hypothetical" as in *Lake*. Given the many, stark factual differences between this case and *Lake*, the court's finding on standing comes as no surprise.

This is especially true given that—unlike this case—the plaintiffs there were candidates who "failed at the polls" and whose "attempts to overturn the election outcome in state have to date been unavailing" with their own elections. 2023 WL 6800710, at *1. Given the *Lake* plaintiffs' claims expressly concerned *election outcomes* rather than simply improper burdens on the individual right to vote, the harm they alleged and sought to prevent *necessarily required* that any future election "manipulation must change the outcome of the election." *Id.* at *4. The harm underlying Plaintiffs' claims here requires no such occurrence. That's because *this* case is not about an election outcome; rather, it is about simply securing each Plaintiff's individual right to vote, irrespective of any outcome of any election.

Finally, in *Lake*, the plaintiffs "claim[ed] no past injury" and "conceded that their arguments were limited to potential future hacking." Plaintiffs' claims and evidence here are not so limited. *Id.* at *2-3. Plaintiffs instead have established here multiple forms of injury, including *both* past and future harm to each of themselves and their individual right to vote in every election in Georgia since the

adoption of the BMD-based system, supported by a massive record that is a far cry from the *Lake* plaintiffs' "conjectural allegations of potential injuries" *only from future hacking.*[3] *Id.* at *2, 4. At least two Plaintiffs here have even shown how they were disenfranchised in past elections in Georgia because of the unconstitutional burdens imposed by the state's voting system. (MSJ Opp at 27-30.) Both this Court and the Eleventh Circuit have confirmed Plaintiffs' standing, and *Lake*—like the other decisions cited in Defendants' summary judgment motions—does not mandate or support a different result. (Dkt. 1630-1, Opp. Ex. 51 at 35-36; Dkt. 1628-13, Opp. Ex. 13 at 17-24.) And the *Lake* decision obviously does not speak to Coalition Plaintiffs' organizational standing at all. It provides no basis to grant Defendants' summary judgment motions and instead highlights the uniquely compelling record Plaintiffs have amassed here to prove up their claims and obtain the relief they seek.

[3] Plaintiffs need only establish a "material risk of harm" from the challenged conduct here, a standard they readily meet with reams of evidence and unrefuted facts. *See Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 933 (11th Cir. 2020) ("The question is whether Muransky has alleged a material risk of harm…."). State Defendants omit that the Ninth Circuit in *Lake* expressly emphasized that this Court's 2018 decision regarding Georgia's DRE system "finding plausible an allegation of a 'future hacking event' is not … contrary" to the *Lake* decision. 2023 WL 6800710, at *4 n.7. In other words, the *Lake* court itself acknowledged that a plausible allegation of a "future hacking event" can be sufficient for standing, just as this Court has held multiple times, including when enjoining Georgia's DRE system in August 2019.

Respectfully submitted this 20th day of October, 2023.

/s/ David D. Cross
David D. Cross (*pro hac vice*)
Mary G. Kaiser (*pro hac vice*)
MORRISON & FOERSTER LLP
2100 L Street, NW, Suite 900
Washington, DC 20037
(202) 887-1500

/s/ Halsey G. Knapp, Jr.
Halsey G. Knapp, Jr.
GA Bar No. 425320
Adam M. Sparks
GA Bar No. 341578
KREVOLIN & HORST, LLC
1201 West Peachtree Street, NW
Suite 3250
Atlanta, GA 30309
(404) 888-9700

/s/ Christian G. Andreu-von Euw
Christian G. Andreu-von Euw
(*pro hac vice*)
THE BUSINESS LITIGATION GROUP, PC
150 Spear Street
San Francisco, CA 94105
(415) 765-6633

Counsel for Plaintiffs Donna Curling, Donna Price & Jeffrey Schoenberg

/s/ Bruce P. Brown
Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

/s/ Russell T. Abney
Russell T. Abney
Georgia Bar No. 000875
WATTS GUERRA, LLP
4 Dominion Drive, Building 3
Suite 100
San Antonio, TX 78257
(404) 670-0355

Counsel for Plaintiff Coalition for Good Governance

/s/ Cary Ichter
Cary Ichter
Georgia Bar No. 382515
ICHTER DAVIS LLC
3340 Peachtree Road NE
Suite 1530
Atlanta, Georgia 30326
(404) 869-7600

Counsel for Plaintiffs William Digges III, Laura Digges, Ricardo Davis & Megan Missett

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing document has been prepared in accordance with the font type and margin requirements of LR 5.1, using font type of Times New Roman and a point size of 14.

/s/ David D. Cross
David D. Cross

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE

I hereby certify that on October 20, 2023, a copy of the foregoing **PLAINTIFFS' RESPONSE TO STATE DEFENDANTS' NOTICE OF SUPPLEMENTAL AUTHORITY** was electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all attorneys of record.

/s/ David D. Cross
David D. Cross